

特 許 協 力 条 約

PCT

国際予備審査報告

(法第12条、法施行規則第56条)
[PCT36条及びPCT規則70]

REC'D 29 JAN 2005

WIPO PCT

| | | |
|--|---|----------------|
| 出願人又は代理人 の書類記号 NT0723PCT | 今後の手続きについては、国際予備審査報告の送付通知(様式PCT/IPEA/416)を参照すること。 | |
| 国際出願番号 PCT/JPO2/06166 | 国際出願日 (日.月.年) 20.06.02 | 優先日 (日.月.年) |
| 国際特許分類(IPC) Int. Cl. ⁷ G09C1/00 H03M13/15 H04L9/30 G06F11/10 | | |
| 出願人(氏名又は名称) 株式会社日立製作所 | | |

- 国際予備審査機関が作成したこの国際予備審査報告を法施行規則第57条(PCT36条)の規定に従い送付する。
- この国際予備審査報告は、この表紙を含めて全部で 3 ページからなる。
☐ この国際予備審査報告には、附属書類、つまり補正されて、この報告の基礎とされた及び/又はこの国際予備審査機関に対してした訂正を含む明細書、請求の範囲及び/又は図面も添付されている。
(PCT規則70.16及びPCT実施細則第607号参照)
この附属書類は、全部で ページである。
- この国際予備審査報告は、次の内容を含む。
I ☒ 国際予備審査報告の基礎
II ☐ 優先権
III ☐ 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
IV ☐ 発明の単一性の欠如
V ☒ PCT35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
VI ☐ ある種の引用文献
VII ☐ 国際出願の不備
VIII ☐ 国際出願に対する意見

| | | |
|---|---|---------|
| 国際予備審査の請求書を受理した日 20.06.02 | 国際予備審査報告を作成した日 10.01.03 | |
| 名称及びあて先 日本国特許庁(IPEA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号 | 特許庁審査官(権限のある職員) 青木 重徳 電話番号 03-3581-1101 内線 3597 | 5M 4229 |

I. 国際予備審査報告の基礎

1. この国際予備審査報告は下記の出願書類に基づいて作成された。(法第6条(PCT 14条)の規定に基づく命令に
応答するために提出された差し替え用紙は、この報告書において「出願時」とし、本報告書には添付しない。
PCT規則70.16, 70.17)

☒ 出願時の国際出願書類

- ☐ 明細書 第 _____ ページ、 出願時に提出されたもの
明細書 第 _____ ページ、 国際予備審査の請求書と共に提出されたもの
明細書 第 _____ ページ、 _____ 付の書簡と共に提出されたもの
- ☐ 請求の範囲 第 _____ 項、 出願時に提出されたもの
請求の範囲 第 _____ 項、 PCT 19条の規定に基づき補正されたもの
請求の範囲 第 _____ 項、 国際予備審査の請求書と共に提出されたもの
請求の範囲 第 _____ 項、 _____ 付の書簡と共に提出されたもの
- ☐ 図面 第 _____ ページ/図、 出願時に提出されたもの
図面 第 _____ ページ/図、 国際予備審査の請求書と共に提出されたもの
図面 第 _____ ページ/図、 _____ 付の書簡と共に提出されたもの
- ☐ 明細書の配列表の部分 第 _____ ページ、 出願時に提出されたもの
明細書の配列表の部分 第 _____ ページ、 国際予備審査の請求書と共に提出されたもの
明細書の配列表の部分 第 _____ ページ、 _____ 付の書簡と共に提出されたもの

2. 上記の出願書類の言語は、下記に示す場合を除くほか、この国際出願の言語である。

上記の書類は、下記の言語である _____ 語である。

- ☐ 国際調査のために提出されたPCT規則23.1(b)という翻訳文の言語
☐ PCT規則48.3(b)という国際公開の言語
☐ 国際予備審査のために提出されたPCT規則55.2または55.3という翻訳文の言語

3. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際予備審査報告を行った。

- ☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際予備審査(または調査)機関に提出された書面による配列表
☐ 出願後に、この国際予備審査(または調査)機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

4. 補正により、下記の書類が削除された。

- ☐ 明細書 第 _____ ページ
☐ 請求の範囲 第 _____ 項
☐ 図面 図面の第 _____ ページ/図

5. ☐ この国際予備審査報告は、補充欄に示したように、補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。(PCT規則70.2(c) この補正を含む差し替え用紙は上記1.における判断の際に考慮しなければならず、本報告に添付する。)

V. 新規性、進歩性又は産業上の利用可能性についての法第12条(PCT35条(2))に定める見解、それを裏付ける文献及び説明

1. 見解

新規性(N)

請求の範囲 _____ 1-7 有
 請求の範囲 _____ 無

進歩性(IS)

請求の範囲 _____ 有
 請求の範囲 _____ 1-7 無

産業上の利用可能性(IA)

請求の範囲 _____ 1-7 有
 請求の範囲 _____ 無

2. 文献及び説明(PCT規則70.7)

請求の範囲1-7

文献1: WO 91/20028 A1 (MASTROVITO, Edoardo)

1991.05.31 全文, FIG. 1-4

には、BCH符号やリードソロモン符号などの誤り訂正符号を計算する場合に、ガロア体 $G(2^m)$ において多項式表現により一般的に表すことができることが示唆されている。

文献2: 斯波万恵, 川村信一, 新保淳; “GF(2^m) 演算及び整数演算を処理可能なハイブリッド・コプロセッサの提案”

1999年暗号と情報セキュリティシンポジウム予稿集,

1999.01.26, Volume II of II,

p. 819-824

には、GF(2^m)で構成される楕円曲線暗号やRSA暗号の様な整数演算型で構成されるものを多倍長積和演算のアーキテクチャを用いて処理できるようなプロセッサが記載されている。

文献3: JP 2001-56640 A (東洋通信機株式会社)

2001.02.27, 全文, 図1-4

には、符号装置や暗号装置に用いられるガロア体上の演算を実現するために必要な積和演算装置が開示されている。

文献4: JP 7-50595 A (株式会社東芝)

1995.02.21 全文, 図1-15

には、演算器、演算回路に入力するパラメータを変化させることで修正シンδροームをユークリッド除算器を利用して求めたり、消失位置多項式を積和演算回路を利用して求めることで、回路の共用化によって回路規模を低減する技術が記載されている。誤り訂正方式と暗号方式とが併用されている技術的背景を鑑みれば、ガロア体上の演算装置について記載されている文献1-3に記載されているものにおいて、文献1に記載されている誤り訂正符号の計算や文献2に記載されている楕円曲線暗号の計算を文献3に記載されている演算装置で実行する際に、文献4に記載されている回路規模の低減技術を考慮して、入力パラメータを変化させることで積和演算装置を共用するように構成することは、当業者にとって自明なことである。



PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Translation

| | | |
|--|--|--------------------------------|
| Applicant's or agent's file reference NT0723PCT | FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416) | |
| International application No. PCT/JP02/06166 | International filing date (day/month/year) 20 June 2002 (20.06.02) | Priority date (day/month/year) |
| International Patent Classification (IPC) or national classification and IPC G09C 1/00, H03M 13/15, H04L 9/30, G06F 11/10 | | |
| Applicant HITACHI, LTD. | | |

- This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
- This REPORT consists of a total of 4 sheets, including this cover sheet.
☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).
These annexes consist of a total of _____ sheets.

- This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

| | |
|---|---|
| Date of submission of the demand 20 June 2002 (20.06.02) | Date of completion of this report 10 January 2003 (10.01.2003) |
| Name and mailing address of the IPEA/JP | Authorized officer |
| Facsimile No. | Telephone No. |

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International Application No.

PCT/JP02/06166

I. Basis of the report

1. With regard to the elements of the international application:*

- ☒ the international application as originally filed
- ☐ the description:
 pages _____, as originally filed
 pages _____, filed with the demand
 pages _____, filed with the letter of _____
- ☐ the claims:
 pages _____, as originally filed
 pages _____, as amended (together with any statement under Article 19
 pages _____, filed with the demand
 pages _____, filed with the letter of _____
- ☐ the drawings:
 pages _____, as originally filed
 pages _____, filed with the demand
 pages _____, filed with the letter of _____
- ☐ the sequence listing part of the description:
 pages _____, as originally filed
 pages _____, filed with the demand
 pages _____, filed with the letter of _____

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item. These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International Application No.
PCT/JP 02/06166

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

| | | | |
|-------------------------------|--------|-----|-----|
| Novelty (N) | Claims | 1-7 | YES |
| | Claims | | NO |
| Inventive step (IS) | Claims | | YES |
| | Claims | 1-7 | NO |
| Industrial applicability (IA) | Claims | 1-7 | YES |
| | Claims | | NO |

2. Citations and explanations

Claims 1 to 7

Document 1: WO 91/20028 A1 (Edoardo Mastrovito), 31 May 1991, entire text, fig. 1-4

Document 1 suggests that when calculating error correction codes such as BCH codes or Reed-Solomon codes, Galois field $GF(2^m)$ elements can in general be represented by polynomial expressions.

Document 2: Kazue Shiba, Shin'ichi Kawamura, Jun Shinbo, "GF(2^m) ensan oyobi seisuu ensan wo shori kanou-na hybrid coprocessor no teian," 1999-nen angou to jouhou security symposium yokoushuu, 26 January 1999, Vol. II of II, pages 819-824

Document 2 discloses a processor which, by using a multiple-length product-sum calculation architecture, can process elliptic curve codes structured over the field $GF(2^m)$ and codes structured using integer algorithms, such as RSA codes.

Document 3: JP 2001-56640 A (Toyo Communication Equipment Co., Ltd.), 27 February 2001, entire text, fig. 1-4

Document 3 discloses a product-sum calculation device needed for performing calculations over a Galois field, said calculations being used in coding devices or encrypting devices.

Document 4: JP 7-50595 A (Toshiba Corp.), 21 February 1995, entire text, fig. 1-15

Document 4 discloses a feature wherein circuits are shared, thus reducing circuit scale, by changing parameters input into a computing unit or a computing circuit and determining correction syndromes using a Euclidean division unit, and deriving the error locator polynomial using a product-sum computing unit. Considering the technical background in which an error correction protocol and an encoding protocol are used together, it would be obvious to a person skilled in the art to take into consideration the feature whereby circuit scale is reduced, disclosed in document 4, and constitute the inventions disclosed in documents 1 to 3 so that, when executing the calculation of error correction codes disclosed in document 1 or the calculation of elliptic curve codes disclosed in document 2 using the calculation device disclosed in document 3, input parameters are changed, allowing a product-sum calculation device to be shared.